САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ – ПРОЦЕССОВ УПРАВЛЕНИЯ

КАФЕДРА МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ

Устинова Светлана Дмитриевна

Выпускная квалификационная работа бакалавра

Технология распределенного реестра в жилищно-коммунальном хозяйстве

Направление 01.03.02

Прикладная математика и информатика

Научный руководитель,
доцент кафедры
математического
моделирования
энергетических систем,
Крылатов А. Ю.

Санкт-Петербург

2018

Содержание

Введение

В эпоху цифрового прогресса каждый день мы наблюдаем зарождение всё новых и новых информационных технологий. Некоторые из них потенциально способны в корне изменить нашу жизнь и повлиять на все без исключения сферы человеческой деятельности.

Благодаря объединению всего современного мира глобальной сетью Интернет уже стерлись национальные, географические границы. Также сетевое пространство осталось за рамками юрисдикции — основного атрибута любого суверенного государства. Экономическая деятельность стала осуществляться путем коммерческих сетей, переплетающихся, в свою очередь, на торговых площадках, на которых поставщики и клиенты, производители и потребители, партнеры и инвесторы, посредники, а также прочие заинтересованные лица управляют своими ценностями, реализуют свои права и привилегии на них.

Одной из наиболее значимых технологий сейчас принято считать технологию Блокчейн (от англ. block chain — цепочка блоков), или, другими словами, технологию распределенного реестра (Distributed Ledger Technology, DLT). Впервые Блокчейн появился в 2009 году в качестве механизма, обеспечивающего децентрализованное, распределенное функционирование инновационной альтернативной платежной системы Биткоин (англ. Bitcoin, bit — бит, coin — монета) и одноименной цифровой валюты. Благодаря открытому коду Биткоина, на данном этапе уже создано множество других криптовалют, в основе каждой из которых лежит собственный блокчейн.

Система Биткоин позволяет осуществлять платежи напрямую от пользователя пользователю без участия третьей доверенной стороны или

центрального органа, например, банка. Биткоин-токены представляют собой виртуальную наличность, фрагмент кода, создаются и удерживаются только в электронном виде, не печатаются подобно фиатным (от лат. fiat — декрет, указание) деньгам, а эмитируются компьютерами, использующими бесплатное программное обеспечение, по всему миру.

Термин «токен» широко применяется в разных сферах, но в области финансов его используют для обозначения «заменителя денег». Электронные жетоны в цифровых платежных системах используются для осуществления трех типов задач: кредитование, продажа акций и монетизация дополнительного сервиса для пользователей сети.

Оригинальный протокол Биткоин не поддерживает возможность выпуска ценных бумаг или предоставления каких-либо сопутствующих услуг. Однако владельцы форков (от англ. fork — вилка) — криптовалют, созданных на основе Биткоина по причине разветвления блокчейна, могут свободно использовать токены. Они выполняю функции внутренней платежной единицы или акций. Такой маркетинговый ход вписывается в концепцию децентрализованной бизнес-модели и позволяет добиться гибкости в решении многих финансовых вопросов.

В данный момент, разглядев весомые преимущества Блокчейна перед устаревшей финансовой системой, экономисты, аналитики и IT-специалисты занимаются изучением возможностей применения технологии за рамками ее первоначального предназначения, а цифровой рынок заполняет множество Блокчейн-стартапов. Список отраслей, которые технология распределенного реестра потенциально способна затронуть в будущем либо уже затронула, не ограничивается финансовым рынком. Блокчейн универсален и способен организовать эффективную деятельность практически в любой сфере жизнедеятельности человека, облегчить координацию всех видов человеческого взаимодействия. Благодаря этой технологии может быть

обеспечена защита интеллектуальной собственности, свободный доступ к медицинской информации, перспективны такие направления, как государственный и корпоративный документооборот, логистика, земельные кадастры. Появление технологии распределенного реестра сравнимо по значимости с зарождением Интернета во второй половине 20-го века.

В этой работе разработана идея внедрения технологии распределенного реестра в отрасли жилищно-коммунального хозяйства, как в одной из самых важных отраслей экономики нашего государства.

Постановка задачи

Поскольку главной идеей данной работы является внедрение технологии Блокчейн в жилищно-коммунальном хозяйстве и построение принципиально новой модели взаимодействия узлов (жилец – поставщик – валидатор) в децентрализованной системе без участия посредников, мы обязаны оценить и предугадать условия, при которых распределенная сеть будет функционировать.

Таким образом, в процессе работы ставится задача моделирования поведения майнеров (валидаторов), так как без участия этих узлов при данной модели консенсуса внедрение технологии распределенного реестра в ЖКХ становится невозможным.

В частности, целью данной работы является нахождение равновесного состояния, при котором майнеры распределяются по блокчейнам таким образом, что отклонение от равновесного положения не выгодно ни для одного из узлов консенсуса.

Обзор литературы

При написании данной работы были использованы научная и учебно-методическая литература, а также статьи, электронные ресурсы и туториалы, описывающие технические аспекты той или иной технологии.

Вопросами децентрализации экономических систем исследователи в области криптографии начали заниматься с конца 20-го века. Впервые применить криптографию в системах расчета предложил программист Вэй Дай (англ. Wei Dai) в 1998 году, описав в своем докладе идею криптовалюты «b-money» [1]. В то же время независимо от него похожие идеи для децентрализованной цифровой валюты «Bit Gold» предложил Ник Сабо (англ. Nick Szabo) [2].

Проблему достижения консенсуса в ненадежной сети («Задача византийских генералов») впервые сформулировал Лесли Лампорт (англ. Leslie Lamport) и в 1982 году предложил рекурсивный алгоритм решения для частного случая, когда количество генералов ограничено и не может динамически изменяться [3]. Первая практическая реализация задачи принадлежит Барбаре Лисков и Мигелю Кастро (Practical Byzantine Fault Tolerance and Proactive Recovery, 2002) [4].

Идея использования алгоритма Proof-of-Work для предотвращения DoS-атак и уменьшения количества спама была описана в 1997 году Адамом Бэком (англ. Adam Back), предложившим собственный механизм под названием Hashcash [5]. Данные работы послужили предпосылками для создания криптовалюты Биткоин, и, соответственно, первого Блокчейна.

Таким образом, основным источником является техническая статья Сатоши Накамото «Биткоин: система цифровой пиринговой наличности» [6], которая и привлекла внимание общественности к такому новому явлению, как цифровая наличность.

Также проблемы консенсуса в распределенных сетях и отказоустойчивости описаны в работе Д.В. Шкурко [7]. Сравнительный анализ алгоритма консенсуса Proof-of-Work и относительно молодого алгоритма Proof-of-Stake проводится в работе [8].

Этапы развития цифровой валюты Биткоин и Блокчейна, перспективы и области возможного применения технологии распределенного реестра в своих книгах описали Мелани Свон [9] и Натаниел Поппер [10].

Также были изучены проблемы отрасли ЖКХ на основании исследований, описанных в работе [11], и учебно-методической литературы [12].

Анализ состояния российской экономики, причин, сдерживающих модернизацию российского общества, и возможных путей этой модернизации проведен в статьях [13,14,15,16,17].

Математические методы оптимизации и методы нелинейного программирования были подробно рассмотрены в работах М. Интрилигатор [18] и Д. Химмельблау [19].

Глава 1. Проблемы отрасли ЖКХ

Жилищно-коммунальное хозяйство является одной из крупнейших отраслей экономики России. По данным Министерства финансов и Государственного комитета Российской Федерации, по статистике расходы российского бюджета в сфере социальной политики сопоставимы с расходами на оборону и превышают затраты на государственную безопасность и государственное управление.

Проблемы жилищно-коммулального сектора являются одними из самых острых и ощутимых для населения и оказывают существенное воздействие на уровень благоустройства страны, социальное положение и уровень жизни россиян. Как и вся экономика страны, отрасль ЖКХ значительно деградировала в последние годы. Для ее поддержания в рабочем состоянии сегодня требуется все больше средств. Тем не менее, в настоящее время более двух третей предприятий, обслуживающих жилищно-коммунальный комплекс, находятся на грани банкротства [12].

Деятельность существующей в настоящее время централизованной системы управления в секторе жилищно-коммунального хозяйства является непрозрачной, а сама сфера сильно подвержена коррупции. Жилищно-коммунальный комплекс претерпевает в данный момент социально-экономический кризис, причинами которого являются:

- устаревшая структура отрасли,
- неэффективная система контроля над распределением ресурсов,
- износ оборудования и слабая техническая база,
- недостаток финансирования,

- малоэффективный механизм установления тарифов,
- монополизм предприятий на предоставление жилищно-коммунальных услуг.

Большую ценность для граждан представляет жилье как важнейший элемент семейной собственности, определяющий имущественный статус семьи. В наше время в условиях постоянной инфляции и обесценивания сбережений для многих семей жилье является единственным ценным материальным имуществом. Его стоимость определяется наличием либо отсутствием коммунальных удобств и общим уровнем комфортности и благоустройства.

Комфортные условия проживания и высокое качество предоставляемых коммунальных услуг есть важнейшие потребности как отдельного человека, так и всего общества в целом. Таким образом, возникает необходимость в реформировании и преобразовании системы жилищно-коммунального хозяйства, переход к совершенно-новой форме взаимодействий.

В марте 2018 года в Государственной Думе в третьем чтении был принят закон, позволяющий потребителям заключать прямые договоры на оказание коммунальных услуг с ресурсоснабжающими организациями. До этого момента, как правило, обслуживанием граждан занималась управляющая компания [11]. Она являлась посредником между клиентом и организациями, предоставляющими те или иные услуги (тепло- и водоснабжение, электроснабжение, поддержание технического состояния дома, капитальный ремонт, вывоз мусора), и именно в руках управляющей компании была сосредоточена власть по распоряжению бюджетом. Этот механизм взаимодействия узлов также изображен на рис.1.

Рисунок 1 – Структура движения средств в сфере ЖКХ.

Жильцы, не имея свободы выбора и альтернатив, регулярно пополняли этот бюджет с целью получения качественного обслуживания, но на практике устоявшаяся система служила отличной основой для нецелевого расходования средств.

Очевидно, для решения вышепоставленных проблем первоначально необходимо обеспечить контроль над исполнением бюджета. К тому же контроль должен осуществляться не вышестоящим органом, имеющим те же недостатки, а должен быть децентрализован [16]. Технология распределённого реестра как нельзя лучше подходит для внедрения в сфере ЖКХ и потенциально способна обеспечить необходимый уровень контроля и прозрачность действий.

Глава 2. Технология распределенного реестра

2.1 О технологии

В общем смысле, термин «реестр» означает список, перечень каких-либо объектов. В экономике реестры представляют собой системы учета экономической деятельности и интересов предприятий. Пример типового реестра представлен в таблице ниже (см. рис. 2).

Вид счета	Денежные средства	Исх.номер	Дебет	Кредит	Баланс
Дата транзакции	Информация о транзакции				
01.01.2018	Расходы за январь	Исх. №1	$100.00		$100.00
01.01.2018	Удержанный налог	Исх. №2		$100.00	($10.00)

Рисунок 2 – Вид типового реестра.

Реестры, которые используют сегодня в экономической деятельности, неэффективны и имеют множество недостатков благодаря централизованному управлению, недостаточной прозрачности функционирования и подверженности неправомерным действиям.

Технология распределенного реестра, или Блокчейн, представляет собой распределенную, децентрализованную книгу учета различных активов, которые могут быть как материальными (недвижимость, машины, здания, земельные участки), так и нематериальными (ценные бумаги, проекты, идеи, интеллектуальная собственность, личная информация, медицинская информация) [9]. Блокчейн является всеобъемлющим и доступным каждому хранилищем историй всех транзакций, с момента его запуска и по настоящий момент.

Достоинствами распределенного реестра являются:

- самообслуживание,
- безопасность,
- независимость от третьих сторон при проведении транзакций,
- необратимость транзакций во времени,
- универсальность,
- прозрачность и невозможность скомпрометировать данные.

Самообслуживание и независимость от третьих сторон возникают по той причине, что в Блокчейне отсутствует центральный администратор. Благодаря встроенным алгоритмам сеть построена таким образом, что ее участники равноправны и одновременно выполняют роль и клиентов, и серверов, подобно архитектуре файлообменной сети BitTorrent [20]. Организация процесса по принципу peer-to-peer (с англ. — равный к равному) позволяет сохранять работоспособность сети при любом количестве и любом сочетании задействованных узлов. Одноранговая сеть может быть публичной, то есть общедоступной, или закрытой, приватной, доступной для использования только ряду лиц.

2.2 Безопасность

Каждый участник сети может генерировать неограниченное количество пар криптографических ключей — открытый и закрытый, а также соответствующий каждой паре криптографический адрес [6]. Приватный ключ представляет собой, как правило, случайное 256-битное число (хэш-алгоритм SHA-256), публичный ключ вычисляется из приватного при помощи необратимой функции умножения на эллиптических кривых (англ. Elliptic Curve Multiplication). Адрес чаще всего является криптографическим

преобразованием открытого ключа (односторонняя хэш-функция) и представляет собой строку из 26-34 буквенно-цифровых символов либо QR-код. Процесс генерации ключей и адресов на примере криптосистемы Биткоин проиллюстрирован на рис.3.

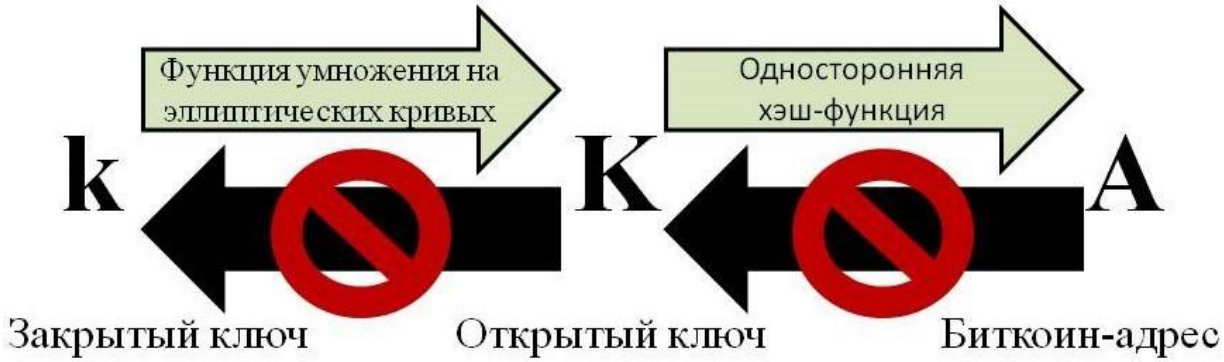

Рисунок 3 – Схема образования ключей и адресов в сети Биткоин.

Подобно адресу электронной почты при отправке сообщений, криптографический адрес используется для проведения транзакций в распределенном реестре. Транзакции подписываются при помощи закрытого ключа, который в свою очередь позволяет системе проверить правомочие действий отправителя. Закрытый ключ подобно паролю от кредитной карты подтверждает право владения пользователем тем или иным активом.

Благодаря криптографии с открытым ключом сеть псевдонимна, безопасна, устойчива к цензуре, пользователи не обязаны делиться приватной информацией и доверять друг другу при совершении транзакций.

В криптосистемах криптографические алгоритмы, а в особенности односторонняя хэш-функция, играют важную роль не только касательно вопросов безопасности, идентификации и аутентификации. На них так же опираются основные принципы алгоритмов достижения консенсуса в децентрализованной сети, которые будут рассмотрены ниже. Чтобы далее перейти к основной теме достижения согласия, остановимся подробнее на определении односторонней функции.

Односторонняя функция — это математическая функция, которая носит односторонний характер касательно своей вычислимости [21]. Это означает, что для такой функции выполняются два условия: относительная легкость вычисления значения функции по заданному аргументу и практическая невозможность вычисления аргумента по известному значению функции.

Определение:

Пусть $\{0,1\}^n$ — множество всех двоичных строк длины n. Тогда функция $f:\{0,1\}^* \to \{0,1\}^*$ является односторонней, если она эффективно вычисляется за полиномиальное время на детерминированной машине Тьюринга, но не существует полиномиальной вероятностной машины Тьюринга, которая обращает эту функцию с более чем экспоненциально малой вероятностью. То есть для любой вероятностной полиномиальной машины M, для любого полинома $p(n)$ и достаточно большого $n \in \mathbb{N}$ выполняется:

$$Pr\,[M\,(f\,(m)) \in f^{-1}(m)] < 1\,/\,p(n),$$

где строка m выбирается случайным образом на множестве $\{0,1\}^n$ в соответствии с законом распределения. Время работы машины M ограничено полиномом от длины искомого прообраза.

Если в независимости от длины аргумента битовая длина значения односторонней функции постоянна и не изменяется, такая функция называется хэш-функцией.

2.3 Достижение консенсуса

Работа Блокчейна децентрализована и распределена между равноправными узлами самой сети, на которых одновременно хранятся и обновляются многочисленные копии «бухгалтерской» книги [6]. Таким

образом, в системе обеспечиваются прозрачность и открытость всех транзакций. Инновационная форма взаимодействия пользователей реестра достигается при помощи встроенного алгоритма достижения консенсуса под названием Доказательство выполнения работы (англ. Proof-of-Work, PoW), который, в свою очередь, решает одновременно две давно известные в сфере компьютерных наук проблемы: проблему двойных трат (англ. Double-spending — двойное расходование) и задачу византийских генералов (англ. Byzantine fault tolerance, BFT).

2.3.1 Проблема двойных трат

Проблема двойных трат возникает по той причине, что электронные устройства способны делать точные копии любой цифровой информации. Таким образом, может возникнуть ситуация, при которой одни и те же активы продаются или покупаются несколько раз. К примеру, атакующий может потратить какую-то сумму денег, а затем распространить собственную ложную версию «бухгалтерской» книги, не включающую эту транзакцию [22]. Решение этой проблемы будет описано ниже.

2.3.2 Задача византийских генералов

Задача византийских генералов (также проблема византийской отказоустойчивости) — это задача поиска наиболее выигрышной стратегии поведения при взаимодействии удаленных абонентов и установления между ними распределенного соглашения в условиях отсутствия доверия.

Задача византийских генералов имеет место быть как в криптологии, так и в вычислительной технике. В вычислительной технике задача византийской отказоустойчивости носит характер мысленного эксперимента, который иллюстрирует проблему синхронизации состояния систем в случае, когда коммуникации считаются надежными, а процессоры – нет [4].

Существует два способа отказа в распределенной вычислительной системе:

- Модель отказа «Остановка»: процессор перестает работать без предупреждения.
- Византийская модель отказа: неисправные процессоры ведут себя неопределенным образом.

Под византийскими отказами могут приниматься любые типы неисправностей, в том числе отказы отдельных компонентов процессоров. Термин «Византийский» впервые был введен в 1978 году Л. Лампортом в его знаковом докладе для такого типа сбоев, в котором в терминах византийских генералов формулируется проблема консенсуса. В 1982 году он же предложил рекурсивный алгоритм решения для ограниченного числа узлов, не изменяющегося динамически[3].

Формулировка задачи:

Византия. Ночь перед сражением с противником. Византийская армия состоит из легионов, каждым из которых командует свой генерал. Также у армии есть главнокомандующий, которому подчиняются генералы.

В то же время, империя находится в упадке, и любой из генералов и даже главнокомандующий могут быть предателями Византии, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее), а именно: «атаковать противника» или «отступать».

Возможные исходы сражения:

1. Если все верные генералы атакуют — Византия уничтожит противника (благоприятный исход).
2. Если все верные генералы отступят — Византия сохранит свою армию (промежуточный исход).
3. Если некоторые верные генералы атакуют, а некоторые отступят — противник уничтожит всю армию Византии (неблагоприятный исход).

Также следует учитывать, что если главнокомандующий — предатель, то он может дать разным генералам противоречивые приказы, чтобы обеспечить уничтожение армии. Следовательно, генералам лучше не доверять его приказам.

Если же каждый генерал будет действовать полностью независимо от других (например, сделает случайный выбор), то вероятность благоприятного исхода весьма низка. Поэтому генералы нуждаются в обмене информацией между собой, чтобы прийти к единому решению.

Алгоритм Б. Лисков и М. Кастро [4] основывается на предыдущих работах по репликации конечных автоматов (Lamport, 1978; Schneider, 1990) и предлагает решение для n реплик, среди которых не более $(n-1)/3$ ошибочны. Обслуживание моделируется как конечный автомат, который реплицируется на разных узлах распределенной системы. Каждая реплика поддерживает состояние обслуживания и выполняет операции обслуживания. Клиенты отправляют запросы на выполнение операций на реплики и BFT-алгоритм гарантирует, что все некачественные реплики выполняют одни и те же операции в одном порядке.

Существует две реплики i и j и, соответственно, два ключа k_{ij} k_{ji} для вычисления MAC-адресов сообщений с одной реплики на другую. Каждая реплика разделяет один секретный ключ с каждым клиентом для

аутентификации связи в обоих направлениях. Сообщения имеют вид $(m)_{\mu ij,}$ где i — отправитель, j — получатель, $(m)_{\alpha i}$ — сообщение от отправителя i для всех пользователей.

Авторы предполагают, что противник вычислительно связан так, что с очень большой вероятностью он не может подорвать криптографические методы и подделать MAC-адрес: если i и j являются неприемлемыми узлами и они никогда не генерировали сообщение $(m)_{\mu ij}$, противник не сможет сгенерировать $(m)_{\mu ij}$ для любого m.

Авторы обозначают множество реплик через R и обозначают каждую реплику, используя целое число из {0, ..., | R | - 1}. | R | = 3 f + 1, где f — максимальное количество реплик, которые могут быть неисправными. Таким образом, число членов сети, достаточное для признания ее правомочной, — это набор с не менее чем 2f + 1 репликами.

Реплики принимают запрос от клиента (лидера) и добавляют его в свой журнал, если они могут его подтвердить. Реплика отправляет ответ на запрос непосредственно клиенту. Ответ имеет форму (REPLY, *v*, *t*, *c*, *i*, *r*) μic, где *v* — текущий номер представления, *t* — метка времени соответствующего запроса, *c* — клиент, *i* — номер реплики, *r* — результат выполнения запрошенной операции.

Клиент ждет сертификаты с ответами от f + 1 реплик с действительными MAC-адресами с одинаковыми метками *t* и *r*, прежде чем принять результат *r*. Поскольку не более *f* реплик могут быть неисправными, это гарантирует, что результат будет действительным.

Если клиент не получит сертификат ответа достаточно быстро, он повторно передает запрос. Если запрос уже обработан, реплики просто повторно передают ответ; реплики запоминают последнее ответное сообщение, которое они отправили каждому клиенту, чтобы включить его

при повторной передаче. Если в течение заданного промежутка времени клиент не присваивает запрос действительному порядковому номеру и в сети не происходит прогресс, в протоколе существует процесс смены лидера. Решение о смене лидера так же, как и решение о признании той или иной информации действительной, принимается большинством узлов.

Этот протокол византийской отказоустойчивости лег в основу механизма достижения консенсуса Proof-of-Work, обеспечивающего функционирование Блокчейн-платформы.

2.3.3 Алгоритм Proof-of-Work

Алгоритм достижения консенсуса Proof-of-Work решает задачу византийских генералов для неограниченного числа узлов с учетом динамического изменения этого числа.

Деятельность, направленную на поддержание и функционирование распределённого реестра, в контексте криптовалют принято называть майнингом (англ. mining — добыча полезных ископаемый). Так называемые узлы консенсуса, или майнеры, группируют новые неподтвержденные транзакции в блок, который вместе со ссылкой на предыдущий блок, номером кошелька майнера и некоторым специальным полем Nonce служат входными данными для односторонней хэш-функции [6].

Nonce не несет смысловой нагрузки для основного сообщения, представляя из себя одноразовый случайный числовой код, предотвращающий атаки двойного расходования. Сообщение подвергается многократному хэшированию (алгоритм SHA-256), а точнее идёт перебор значений поля Nonce до тех пор, пока не будет найден хэш, удовлетворяющий заранее заданным условиям. На каждом новом этапе значение поля Nonce увеличивается на единицу. Алгоритм действий подробно описан на рис. 4.

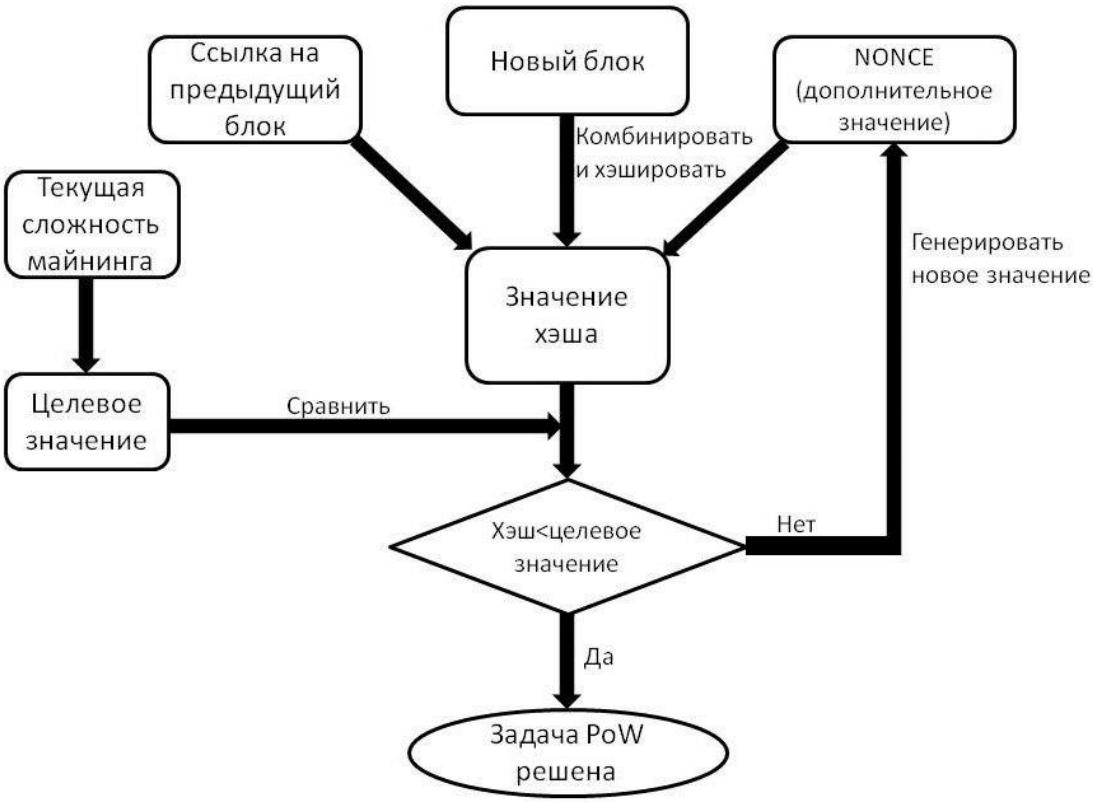

Рисунок 4 – Алгоритм достижения консенсуса Proof-of-Work.

2.4 Эмиссия и сложность майнинга

Условия, которым должен соответствовать найденный хэш, определяются текущей сложностью майнинга (англ. difficulty). Сложность майнинга — это параметр, который компенсирует неуклонный прирост новых узлов консенсуса и вычислительных мощностей. Сложность = 1 соответствует достижимой цели, в которой тридцать два первых бита нули. Соответственно, для генерации подписи блока нужно в среднем ($2^{32} * $ сложность) попыток. В сети Биткоин на данный момент текущей сложности удовлетворяет хэш, в котором 49 первых битов равны нулю, а последующие 23 бита хэша меньше 6A93B3 [10].

По мере увеличения численности вовлеченных в сеть узлов-майнеров сложность майнинга пропорционально вырастает, и соответственно, с уменьшением количества задействованных узлов консенсуса, задача

облегчается. К примеру, в протоколе Биткоина программно заложено изменение сложности вычислений через каждые 2016 блоков для того, чтобы сохранялось одинаковое среднее значение времени нахождения нового блока, равное 10-ти минутам [23].

Первый узел, нашедший нужное значение Nonce, добавляет блок в цепочку, а все остальные узлы с помощью очередной операции хэширования могут с лёгкостью проверить результат выполненной им работы и подтвердить его: необходимо произвести всего один вызов хэш-функции, чтобы проверить валидность хэша. Таким образом, консенсус между участниками сети, не доверяющими друг другу, достигается путем математических вычислений и задействования больших вычислительных мощностей. Механизм Proof-of-Work защищает сеть от атак двойного расходования и других возможных атак, поскольку злоумышленник обязан выполнять те же математические задачи наряду с остальными участниками сети, и, следовательно, атака будет успешной только в том случае, если ему удастся завладеть достаточным количеством вычислительных ресурсов [6].

Кроме того, протоколы большинства криптовалют построены таким образом, что транзакция окончательно подтверждается только по завершении работы над некоторым количеством последующих блоков в цепочке [9]. К примеру, ПО Биткоина не подтверждает перевод, пока не будут найдены следующие 6 блоков, благодаря чему транзакции практически невозможно проводить в обратном направлении. Для отмены транзакции потребуется пересчитывать все блоки, созданные после блока, содержащего данную транзакцию, заново. Допустим, в данный момент идет работа над добычей блока № 85, один из майнеров хочет изменить транзакцию в блоке № 71, для этого ему необходимо изменить транзакцию в блоке 71 и заново пересчитать блоки 71-85, то есть найти новые хэши, удовлетворяющие условиям. К тому же, эту работу нужно проделать до того, как другие участники сети найдут

блок № 85 и последуют дальше, что практически невозможно с точки зрения задействующихся мощностей. Этот аспект является очень важным в том смысле, что Блокчейн позволяет фиксировать достоверную информацию в открытой и неизменной цепочке транзакций и сводит к нулю все попытки злоумышленников подделать эту информацию.

Майнер, добавивший новый блок в цепочку, получает вознаграждение в виде эмитированной криптовалюты. Количество выпускаемой криптовалюты, как правило, ограничено программно и не превышает какое-то конкретное значение. К примеру, сумма всех эмитированных монет в рамках системы Биткоин не будет превышать 21 миллион [6]. Выпуск этой криптовалюты представляет собой убывающую геометрическую прогрессию. Награда за блок рассчитывается как поразрядное смещение 64-битного целого числа со знаком вправо, т.е. производится деление на два и округление в меньшую сторону. Изначально, награда за новый блок, добавленный в цепочку, составляла 50 биткоинов. Таким образом, в соответствии с протоколом криптовалюты каждый раз, когда в оборот выпускается половина от оставшейся суммы монет, примерно каждые 4 года или каждые 210000 блоков, размер вознаграждения уменьшается вдвое, что, в итоге, приведет к полному завершению эмиссии биткоина в 2041 году.

После того, как вся криптовалюта будет эмитирована, планируется обеспечивать деятельность системы с помощью комиссионного поощрения майнеров. Ограниченная эмиссия и программируемая сложность майнинга обеспечивают стабильность системы, равномерный прирост криптовалюты и устойчивость к инфляции.

Глава 3. Применение технологии распределенного реестра в ЖКХ

3.1 Разработанная платформа

Была разработана платформа на базе технологии Блокчейн, основу которой составили узлы трех видов: поставщики, жильцы и валидаторы. В нашей модели мы полностью уходим от необходимости присутствия управляющей компании. Поставщиками являются организации, предоставляющие жилищно-коммунальные услуги. Здесь принципы Блокчейна также позволяют решить проблему монополизации и расширяют диапазон доступных услуг. Жильцы заключают контракты с поставщиками напрямую. Валидаторы — это смарт-контракты либо любые доверенные лица, они же майнеры, которые выполняют функцию контроля над совершаемыми транзакциями, пресекая попытки расходования бюджета не по назначению и обеспечивая функционирование всей платформы. Схема взаимодействия узлов показана на рис.5.

Рисунок 5 – Распределения ролей ЖКХ в Блокчейн-платформе.

На почве этой идеи возникло два основных вопроса: каким необходимым количеством валидаторов-майнеров должна быть обеспечена сеть для корректной работы и при каких условиях валидаторам выгодно будет поддерживать деятельность в сети?

Существует два способа улучшения доходности майнинга: увеличение прибыльности и снижение расходов. Прибыль складывается из наград за утвержденные блоки и комиссии за проведение включенных в них транзакций. Расходы возникают из потребности оплачивать электричество, оборудование, зарплаты сотрудников, аренду офисов и подобные издержки.

С уменьшением прибыльности майнинга уменьшается поток майнеров, готовых предоставлять свои вычислительные ресурсы. В рамках данной платформы мы предполагаем, что майнеры самостоятельно выбирают, к какому реестру подключиться из соображений прибыльности. Чем больше майнеров подключается к той или иной системе, тем меньше прибыль каждого из них.

Смоделируем ситуацию: N — некоторое множество майнеров-валидаторов, потенциально готовых подключиться к тому или иному блокчейну. D — искомое, конечное количество майнеров, которое в итоге подключится.

$$\sum_{i \in N} x_i = D$$

К i-му блокчейну подключается $x_i \in [0, N]$ майнеров.

Определим функцию прибыльности $g_i(x_i)$ одного майнера, работающего над i-м реестром, к которому суммарно подключилось x_i майнеров, как убывающую функцию.

Основной интерес представляет вопрос, какое количество майнеров в итоге подключится и к какому Блокчейну. Решением задачи является

равновесное состояние, в котором валидаторы распределяются между разными реестрами таким образом, что покидать это положение каждому из них становится невыгодно. Любое отклонение от равновесного состояния влечет за собой уменьшение прибыли.

3.2 Математическая модель

Предположим, что у нас есть набор Блокчейн-платформ с набором возможных майнеров N. Каждый из N майнеров готов предоставить свои вычислительные ресурсы.

Рассмотрим функцию спроса:

$$D = p(p^*),$$

где p^* — равновесная прибыль.

$$\max_{x,D}\left(\sum_{i\in N}\int_0^{x_i} g_i(u)du - \int_0^{D} p^{-1}(v)dv\right) \tag{1}$$

при условии

$$\sum_{i\in N} x_i = D, \tag{2}$$

$$x_i \geq 0 \quad \forall i \in N. \tag{3}$$

Лагранжиан:

$$L = \sum_{i\in N}\int_0^{x_i} g_i(u)du - \int_0^{D} p^{-1}(v)dv + p^*\left(D - \sum_{i\in N} x_i\right) + \sum_{i\in N} x_i\eta_i \tag{4}$$

Продифференцируем:

$$\frac{\partial L}{\partial x_i} = g_i(x_i) - p^* + \eta_i = 0 \quad \forall i \in N \tag{5}$$

$$\frac{\partial L}{\partial D} = -p^{-1}(D) + p^* = 0 \tag{6}$$

Далее рассмотрим частный случай (линейная функция прибыли):

$$g_i(x_i) = a_i - b_i x_i \quad \forall i \in \{1, n\} \tag{7}$$

Решение данной модели состоит в нахождении вектора распределения майнеров $x = (x_1, \dots, x_n)$ по блокчейнам с учетом эластичности спроса D от оптимальной равновесной прибыли p^*.

В итоге, в предложенных обозначениях (7) математическая задача (1) – (3) преобразуется таким образом:

$$Z(x^*, D^*) = \max_{x,D} \left\{ \sum_{i=1}^{n} \int_0^{x_i} (a_i - b_i u_i) du - \int_0^{D} p^{-1}(v) dv \right\}, \tag{8}$$

$$\sum_{i=1}^{n} x_i = D, \tag{9}$$

$$x_i \geq 0, \quad \forall i \in \{1, n\} \tag{10}$$

Перенумеруем реестры с учетом преобразований:

$$a_1 \geq \cdots \geq a_n \tag{11}$$

Справедлива следующая ***теорема:***

При выполнении условия (11) в задаче (8) – (9) конкурентное равновесие достигается только тогда, когда распределение майнеров по блокчейнам:

$$x_i = \begin{cases} \dfrac{a_i}{b_i} - \dfrac{1}{b_i} p^*, & \text{при } i \leq k \\ 0, & \text{при } i > k \end{cases} \quad i \in \{1, n\}, \tag{12}$$

где p^* находится, как

$$p^* = \frac{\sum_{i=1}^{k} \frac{a_i}{b_i}}{\frac{1}{r} + \sum_{i=1}^{k} \frac{1}{b_i}} \tag{13}$$

В данной модели, учитывая ограничение (9), найти количество используемых реестров k можно из уравнения:

$$\sum_{i=1}^{k} \frac{a_i - a_k}{b_i} < \frac{\sum_{i=1}^{k} \frac{a_i}{b_i}}{1 + r\sum_{i=1}^{k} \frac{1}{b_i}} \tag{14}$$

при этом

$$D = \frac{p^*}{r} \tag{15}$$

Доказательство.

Оптимальная равновесная прибыль является множителем Лагранжа, соответствующим ограничению (9) задачи (8) – (10):

$$L = \sum_{i=1}^{n} \int_0^{x_i} g_i(u)du - \int_0^{D} p^{-1}(v)dv + p^* \left(D - \sum_{i=1}^{n} x_i \right) + \sum_{i=1}^{n} \eta_i(x_i),$$

где $\eta_i \geq 0, i \in \{1, n\}$ – множители Лагранжа, соответствующие ограничению (10) задачи (8) – (10). Дифференцируя данный Лагранжиан по D и x_i, $i \in \{1, n\}$ и приравнивая к нулю, получаем:

$$g_i(x_i) = p^* - \eta_i, \;\; i \in \{1, n\} \tag{16}$$

$$p^* = p^{-1}(D) = rD$$

Из условий Куна-Таккера воспользуемся условием дополняющей нежесткости к уравнению (16):

$$\eta_i x_i = 0,$$

из которого следует, что если $x_i > 0$, то $\eta_i = 0$, если $x_i = 0$, то $\eta_i \geq 0$.

Отсюда,

$$p^* \begin{cases} = a_i - b_i x_i, & \text{при } x_i > 0, \\ \leq a_i, & \text{при } x_i = 0, \end{cases} \quad \forall i \in \{1, n\}$$

Выражаем x_i и получаем

$$x_i = \frac{a_i - p^*}{b_i} \tag{17}$$

Далее подставляя последнее выражение в (9) и выражая из него спрос, находим

$$D = -p^* \sum_{i=1}^{k} \frac{1}{b_i} + \sum_{i=1}^{k} \frac{a_i}{b_i} = \frac{p^*}{r}$$

После преобразований получаем (13), и следом (12).

Теорема доказана.

3.3 Программная реализация

Целью данной работы являлся не только поиск аналитического решения, но и его успешное практическое применение. Для решения задач технических вычислений был использован пакет программы Wolfram Mathematica 11.1. Полученное компьютерное решение было применено к экспериментальным данным. Остановимся на них подробнее.

Имеется 10 вакантных блокчейнов, к которым могут присоединиться майнеры или, другими словами, 10 вариантов вложиться, каждый из которых имеет прибыльность $g_i(x_i) = a_i - b_i x_i$. Заданы коэффициенты a_i и b_i в виде векторов $a = [6; 5; 9; 10; 6; 10; 8; 7; 5; 7]$ и $b = [0.1; 0.5; 0.3; 0.4; 0.3; 0.1; 0.2; 0.5; 0.3; 0.1]$ соответственно. Также задан коэффициент зависимости спроса от прибыльности в виде вектора $r = [0.1; 0.2; 0.5; 2]$.

Далее n — это количество возможных вариантов подключения майнеров к блокчейнам, $n \in [2,10]$. К примеру, $n = 2$ означает, что 2 из 10 блокчейнов могут быть задействованы, $n = 3$ — 3 блокчейна из 10 и т.д.

k — количество блокчейнов, которые в итоге майнеры будут использовать.

Результаты работы программной реализации для заданных экспериментальных данных представлены в таблицах 1–4.

n	2	3	4	5	6	7	8	9	10
k	2	3	4	5	3	4	5	5	6
D	31.8182	39.4737	44.9102	46.5241	60	63.2432	63.6548	63.6548	65.1362
p*	3.18182	3.94737	4.49102	4.65241	6	6.32432	6.36548	6.36548	6.51362

Таблица 1 – Результаты работы программы для r = 0.1.

Для n = 2: $x_1 = 28.1818,\ x_2 = 3.6363$, $g_i(x_i)$ = 3.18182.

Для n = 3: x_1 = 16.8421, x_2 = 20.5263, x_3 = 2.10526, $g_i(x_i)$ = 3.94737.

Для n = 4: x_1 = 13.7725, x_2 =15.0299, x_3 = 15.0898, x_4 = 1.01796, $g_i(x_i)$ = 4.49102

Для n = 5: x_1 = 13.369, x_2 = 14.492, x_3 = 13.4759, x_4 = 4.49198, x_5 = 0.695187, $g_i(x_i)$ = 4.65241.

Для n = 6: x_1 = 10, x_2 = 40, x_3 = 10, $g_i(x_i)$ = 6.

Для n = 7: x_1 = 9.18919, x_2 = 36.7568, x_3 = 8.91892, x_4 = 8.37838, $g_i(x_i)$ = 6.32432.

Для n = 8, n = 9: x_1 = 9.08629, x_2 = 36.3452, x_3 = 8.78173, x_4 = 8.17259, x_5 = 1.26904, $g_i(x_i)$ = 6.36548.

Для n = 10: x_1 = 8.71595, x_2 = 34.8638, x_3 = 8.28794, x_4 = 7.43191, x_5 = 0.972763, x_6 = 4.86381, $g_i(x_i)$ = 6.51362.

N	2	3	4	5	6	7	8	9	10
K	2	3	3	4	3	4	4	4	4
D	20.5882	24.5902	27.6	27.931	37.2	37.7419	37.7419	37.7419	37.7419
p*	4.11765	4.91803	5.52	5.58621	7.44	7.54839	7.54839	7.54839	7.54839

Таблица 2 – Результаты работы программы для r = 0.2.

Для n = 2: $x_1 = 18.8235$, x_2 = 1.76471, $g_i(x_i)$ = 4.11765.

Для n = 3: x_1 = 13.6066, x_2 = 10.8197, x_3 = 0.163934, $g_i(x_i)$ = 4.91803.

Для n = 4: x_1 = 11.2, x_2 = 11.6, x_3 = 4.8, $g_i(x_i)$ = 5.52.

Для n = 5: x_1 = 11.0345, x_2 = 11.3793, x_3 = 4.13793, x_4 = 1.37931, $g_i(x_i)$ = 5.58621.

Для n = 6: x_1 = 6.4, x_2 = 25.6, x_3 = 5.2, $g_i(x_i)$ = 7.44.

Для n = 7, n = 8, n = 9, n = 10: x_1 = 6.12903, x_2 = 24.5161, x_3 = 4.83871, x_4 = 2.25806, $g_i(x_i)$ = 7.54839.

N	2	3	4	5	6	7	8	9	10
k	1	2	2	2	3	3	3	3	3
D	10	11.7391	14.0426	14.0426	17.3832	17.3832	17.3832	17.3832	17.3832
p*	5	5.86957	7.02128	7.02128	8.69159	8.69159	8.69159	8.69159	8.69159

Таблица 3 – Результаты работы программы для r = 0.5.

Для n = 2: x_1 = 10, $g_i(x_i)$ = 5.

Для n = 3: x_1 = 10.4348, x_2 = 1.30435, $g_i(x_i)$ = 5.86957.

Для n = 4, n = 5: x_1 = 7.44681, x_2 = 6.59574, $g_i(x_i)$ = 7.02128.

Для n = 6, n = 7, n = 8, n = 9, n = 10: x_1 = 3.27103, x_2 = 13.0841, x_3 = 1.02804, $g_i(x_i)$ = 8.69159.

N	2	3	4	5	6	7	8	9	10
K	1	1	2	2	2	2	2	2	2
D	2.85714	3.91304	4.34211	4.34211	4.80769	4.80769	4.80769	4.80769	4.80769
p*	5.71429	7.82609	8.68421	8.68421	9.61538	9.61538	9.61538	9.61538	9.61538

Таблица 4 – Результаты работы программы для r = 2.

Для n = 2: x_1 = 2.85714, $g_i(x_i)$ = 5.71429.

Для n = 3: x_1 = 3.91304, $g_i(x_i)$ = 7.82609.

Для n = 4, n = 5: x_1 = 3.28947, x_2 = 1.05263, $g_i(x_i)$ = 8.68421.

Для n = 6, n = 7, n = 8, n = 9, n = 10: x_1 = 0.961538, x_2 = 3.84615, $g_i(x_i)$ = 9.61538.

Фрагмент программного кода представлен в приложении 1 на рисунке 6.

Заключение

Основной целью данной работы являлось исследование условий, при выполнении которых внедрение технологии распределенного реестра в сферу жилищно-коммунального хозяйства становится эффективным, поскольку отрасль ЖКХ является наиболее нуждающейся в коренном реформировании.

Для достижения этой цели были сформулированы задачи:

1. Построение математической модели, описывающей оптимальное распределение майнеров по Блокчейн-платформам, с учетом эластичности спроса в зависимости от прибыльности;
2. Программная реализация аналитического решения.

Для решения поставленных задач использовались модели и методы нелинейной оптимизации. В результате работы было найдено оптимальное равновесное состояние системы, в котором каждый майнер занимает выгодное с точки зрения прибыльности положение и обеспечивает функционирование всей сети. Программная реализация осуществлялась с помощью пакета программы Wolfram Mathematica 11.1.

Актуальность данной темы обсуждается на государственном уровне. На данный момент работа по направлению внедрения технологии распределенного реестра ведется в разных экономических сферах государства. С целью улучшения уровня защиты данных и обеспечения их максимальной прозрачности, Центробанк РФ планируется перенести Систему передачи финансовых сообщений (СПФС) на Блокчейн-платформу уже в 2019 году. Основная концепция Блокчейна позволяет организовать менее затратную и более эффективную деятельность в любом масштабе. Неоспоримые достоинства технологии способны вывести на новый уровень как экономику в целом, так и отдельные ее отрасли.

Список литературы

1. Dai W. Alternative b-money creation [Электронный ресурс]: URL: http://www.weidai.com/bmoney.txt (дата обращения: 05.02.18)

2. Szabo N. Bit gold [Электронный ресурс]: URL: http://unenumerated.blogspot.ru/2005/12/bit-gold.html

3. Lamport L. The Byzantine Generals Problem (with M. Pease and R. Shostak) // ACM Transactions on Programming Languages and Systems, Vol. 4, No 3, July 1982. P. 382–401.

4. Liskov B., Castro M. Practical Byzantine Fault Tolerance and Proactive Recovery // ACM Transactions on Computer Systems, Vol. 20, No. 4, November 2002. P. 398–461.

5. Back A. Hashcash — A Denial of Service Counter-Measure [Электронный ресурс]: URL: http://www.hashcash.org/papers/hashcash.pdf (дата обращения: 15.01.18)

6. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]: URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 10.03.18).

7. Шкурко Д.В. Отказоустойчивость в распределенных сетях: проблемы консенсуса // Проблемы интеллектуализации и качества систем информатики, 2006. С. 229–248.

8. BitFury Group. Proof of Stake versus Proof of Work [Электронный ресурс]: URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

9. Свон М. Блокчейн. Схема новой экономики. М.: Олимп-Бизнес, 2017. 240 с.

10. Поппер Н. Цифровое золото. Невероятная история Биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново. М.: Вильямс, 2016. 350 с.

11. Соколова С.А., Борисова К.В. Проблемы жилищно-коммунального хозяйства как индикатор состояния общества. // Фундаментальные исследования, № 11-4, 2016. С. 870 – 874.
12. Кондратьева М. Н. Организация и управление жилищно-коммунальным хозяйством. Учебное пособие для студентов высших учебных заведений. Ульяновск: УлГТУ, 2009. 160 с.
13. Абрамов В.Л. Конкурентоспособность экономики России: современное состояние и стратегия развития // Экономика, статистика и информатика, №2, 2012. С. 3 – 7.
14. Антипьев А.Г. О путях модернизации экономики и современного российского общества // Труд и социальные отношения, № 1, 2011. С. 3–11.
15. Антипьев А.Г. Модернизация «архаичного» российского общества: состояние и проблемы // Вестник Пермского университета, № 3, Пермь, 2010. С. 96 – 103.
16. Антипьев А.Г. О причинах, сдерживающих модернизацию российского общества // Вестник Вятского государственного университета, №1, 2013. С. 6 –11.
17. Королюк Е. Современная экономика России: стратегическая ориентация и хозяйственное пространство // Проблемы теории и практики управления, № 4, 2011. С. 18-26.
18. Интрилигатор М. Математические методы оптимизации и экономическая теория. М.: Прогресс, 1975. 604 с.
19. Химмельблау Д. Прикладное нелинейное программирование. М.: Мир, 1975. 536 с.
20. [Электронный ресурс]: URL: https://www.campaignlive.co.uk/article/just-bit-torrent-file-distributes-content-blockchain-distributes-trust/1350075 (дата обращения: 25.05.2018)

21. Catalano D., Fiore D., Gennaro R., Vamvourellis K. Algebraic (Trapdoor) One-Way Functions and their Applications [Электронный ресурс]: URL: https://eprint.iacr.org/2012/434.pdf (дата обращения: 13.04.2018)

22. Capkun S. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin [Электронный ресурс]: URL: https://eprint.iacr.org/2012/248.pdf (дата обращения: 20.04.2018)

23. [Электронный ресурс]: URL: https://bravenewcoin.com/news/number-of-bitcoin-miners-far-higher-than-popular-estimates/ (дата обращения: 02.04.2018)

Приложение 1

```
#!/usr/bin/env wolframscript
g=0
For[pos=2,pos≤10,pos++,
If [pos==2,For [i=1,i≤pos,i++,AA=AA+(a2[i]-a2[pos])/b2[i];DD1=DD1+a2[i]/b2[i];
DD2=DD2+1/b2[i]];
DD=DD1/(1+r*DD2);
Print["для случая 2  ", AA];
Print["для случая 2 D ", DD];
p=DD*r;
Print["для случая 2 p* ", p];
For [i=1,i≤pos,i++,x=a2[i]/b2[i]-p/b2[i];
g=a2[i]-b2[i]*x;
Print["x", i, "=", x];
Print["g", i,"=", g]];
g=0;
p=0;
x=0;
AA=0;
DD1=0;
DD2=0;
DD=0,
If [pos==3,For [i=1,i≤pos,i++,AA=AA+(a3[i]-a3[pos])/b3[i];
DD1=DD1+a3[i]/b3[i];
DD2=DD2+1/b3[i]];
DD=DD1/(1+r*DD2);
Print["для случая 3  ", AA];
Print["для случая 3 D ", DD];
p=DD*r;
Print["для случая 3 p* ", p];
For [i=1,i≤pos,i++,x=a3[i]/b3[i]-p/b3[i];
g=a3[i]-b3[i]*x;
Print["x", i, "=", x];
```

Рисунок 6 – Фрагмент программного кода.